UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/732,808	12/11/2003	Benoit De Boursetty	324-162	5873

7590 05/09/2008

LOWE HAUPTMAN GILMAN & BERNER, LLP
Suite 300
1700 Diagonal Road
Alexandria, VA 22314

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/732,808	DE BOURSETTY ET AL.	
	Examiner	Art Unit	
	HARRIS C. WANG	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/28/2008 has been entered.

Response to Arguments

The Applicant has argued that “the Sudia delegation certificate does not include the second information of at least a delegator (e.g. the primary user’s identity) (pg. 9 of Remarks)." This is contrasted by the Sudia’s description of the delegation certificate “The certificate, signed by the primary user’s signature… (Column 27, lines 54).” It is understood in the cryptographic art that a digital signature is considered information describing one’s identity.

The Applicant next argues that “the steps of this preferred approach differ from the steps defined by claim 1 because the first member (delegate) does not prepare and sign a request to be transmitted to a delegator’s smart card (pg. 9 Remarks).”

Nowhere in the claim language does the Applicant exclude the preferred approach of Sudia, so this argument is considered spurious.

The Applicant next argues that “In Sudia the signature of the document does not depend on first and second information concerning the first member and the second member included in the delegation certificate or substitution certificate.

This is contrasted by the description of the delegation certificate that includes the primary user's signature as well as the delegates key. The terms "first information" and "second information" is broad enough to support the delegation certificate of Sudia.

The Applicant argues that "Sudia does not use a delegation means similar to the delegation credential service provider in Brickell to issue first and second information , or a delegation certificate or a substitution certificate. Therefore, those skilled in the art would not have combined Brickell and Sudia. Remarks Pg 9).”

The prior art Brickell included each element claimed (Delegator, Delegate, Delegation Means, User, Delegation Certificate, Signature) and one of ordinary skill in the art could have combined the elements as claimed by known methods (Digital Signing by the delegate, as taught by Sudia) and that in combination, each element merely would have performed the same function as it did separately. One of ordinary skill in the art would have recognized that the results of the combination were predictable.

As a final note, although the Applicant has clarified what he intends the claimed limitations to mean in the Remarks (e.g. first member, second member, first information, second information) none of these descriptions appear in the claim language. Therefore all arguments regarding these terms will be considered using the broadest reasonable interpretation of these limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-8, 10-17, 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brickell (US20030145223) in view of Sudia (5825880).

Regarding Claims 1 and 10,

Brickell teaches the system and method of delegating signing of predetermined data by a given one of M first members mandated by N second members, M and N being integers of which one is equal to 1 and the other is at least equal to 2 *("we refer to a user who is engaged in a delegation relationship as either a delegator who assigns a delegation authority or a delegate who is assigned a delegation authority" Paragraph [0022]", The Examiner interprets M first members as the delegates, and the Examiner further interprets the N second members as the delegators),* the given first member having a terminal *("the processing described below may be performed by a…general purpose computer" Paragraph [0021])* containing first information on said given first member *("A user…with appropriate credential information" Paragraph [0023]),* said method comprising the following steps:

Reading first information on said M first members and second information on said N second members in delegation means responsive to a first identifier of said given first member included in said first information and transmitted by said terminal to said delegation means, *("A user who requests a delegation service may provide information relevant to the delegation such as the identities of the delegator and the delegate" Paragraph [0044]).* The Examiner interprets the DCSP (Delegate Credential Service Provider, shown in Fig. 7, as the delegation means. The Examiner interprets reading first and second information as the identities of the delegator and delegate.

Brickell further teaches applying predetermined data, said first information, said second information, and a first private key of said given first member to a cryptographic algorithm implemented in said terminal to produce a signature. *("The delegate…requests…as service from the relying party. The delegate signs this…with his private signature key" Paragraph [0033]).* It is inherent that the private signature key is for producing a signature. It has already been cited above that request requires relevant information needs to be produced including the identities of the delegator and delegate (1st information and 2nd information). It is inherent that if a delegate is used there must be a predetermined data selected for delegation.

Brickell further teaches transmitting said predetermined data, said first information, said second information, and said signature to any user terminal interested in said predetermined data. *("With the returned credential information, the relying party authenticates the delegate….based on the authentication result, the relying part generates…a service response and sends…the response back to the delegate" Paragraph [0033]).* The Examiner interprets transmitting the data was the response being sent back.

While Brickell teaches the delegation means reading in the delegation information, Brickell does not explicitly teach reading from the terminal first and second information, or transmitting predetermined data from the delegate to any user terminal.

Sudia teaches a multi-step digital signature method which involves "an original authorizing agent ("primary user") to issue a specialized "delegation" certificate to substitute authorizing agent ("delegate"). The certificate, signed by the primary user, would identify the delegate and the delegate's public signature verification key…A

delegate, using his/her personal smart card, would sign a document using the delegate's personal signature key and would attach the delegation certificate. Resulting documents would be signed by the delegate, not the primary user, and a document recipient must undertake additional steps to verify the delegate's signature and the delegate certificate." (Column 27, lines 51-62) The Examiner interprets the delegate receiving the delegation certificate as receiving the first and second information, and the document recipient as the user that the data is transferred to.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the delegation means which includes the identities of the delegators and delegates, as taught by Brickell, with the delegate signing method as taught by Sudia.

The prior art Brickell included each element claimed (Delegator, Delegate, Delegation Means, User, Delegation Certificate, Signature) and one of ordinary skill in the art could have combined the elements as claimed by known methods (Digital Signing by the delegate, as taught by Sudia) and that in combination, each element merely would have performed the same function as it did separately. One of ordinary skill in the art would have recognized that the results of the combination were predictable.

The cited art above also teaches the apparatus associated with the method above, in particular the given M first members for delegating the signing, the N second members for mandating the signing *("we refer to a user who is engaged in a delegation*

relationship as either a delegator who assigns a delegation authority or a delegate who is assigned a delegation authority" Paragraph [0022]", The Examiner interprets M first members as the delegates, and the Examiner further interprets the N second members as the delegators). The terminal which has a cryptographic capabilities. *("the processing described below may be performed by a…general purpose computer" Paragraph [0021]) ("The delegate…requests…as service from the relying party. The delegate signs this…with his private signature key" Paragraph [0033])*

Regarding Claims 2, 11

Brickell and Sudia teach the system and method claimed in claim 1, wherein said second information on a second member comprises at least an identifier of said second member. *("A user who requests a delegation service may provide information relevant to the delegation such as the identities of the delegator and the delegate" Paragraph [0044])*

Regarding Claims 3-4, 12-13

Brickell and Sudia teach the method claimed in claim 1 wherein said second information on a second member further comprises a public key of said second

member, also wherein said second information on a second member further comprises an electronic certificate of said second member.

("A user's digital certificate may comprise…a user's public key" Paragraph [0034], Brickell)

Regarding Claim 5, 14

Brickell and Sudia teach the method claimed in claim 1 wherein said first information on a first member comprises an electronic certificate of said first member. *(Fig. 5, Delegation Certificate, Brickell)*

Regarding Claim 6, 15

Brickell and Sudia teach the method claimed in claim 1. Brickell further teaches wherein said integer M (delegate) is equal to 1 and said integer N (delegator) is at least equal to 2. *("The DCSP interfaces with both delegates 210a…220b and delegators 210…220a…The DCSP comprises a service registration interface that interfaces with users (delegates and delegators) for subscription and registration purposes" Paragraph [0042]) ("A delegate may refer to any user. For example, a user who may be a delegator in a separate delegation relationship may independently send a service request to the relying party" Paragraph [0033], Brickell)*

The above references teach that there are groups of delegates and delegators, where the DCSP assigns the relations between them. The references further teach that an user may either a delegator or a delegate or both. Therefore it is inherent that Brickell anticipates where the integer M is equal to 1 and integer N is at least equal to 2.

Regarding Claim 7, 16

Brickell and Sudia teach the method claimed in claim 1. Brickell further teaches ("The DCSP interfaces with both delegates 210a…220b and delegators 210…220a" Paragraph [0042]), wherein said integer N (delegator) is equal to 1 and said integer M (delegate) is at least equal to 2 ("a relying party authorizes services to a plurality of delegates." Paragraph [0022], Brickell)

Regarding Claim 8, 17

Brickell and Sudia teach the method claimed in claim 1 wherein said M first members and said N second members constitute a group of members. ("The DCSP interfaces with both delegates 210a…220b and delegators 210…220a" Paragraph [0042], Brickell)

Regarding Claims 19-20,

Brickell and Sudia teach the system and method of Claim 1. Brickell and Sudia further teach predetermined data, first information, second information, and a first private key to produce a signature. Figure 5 of Brickell teaches delegate identity, delegator identity, which the Examiner interprets as 1st and 2nd information. Column 27 of Sudia teaches predetermined data ("document") and a private key ("delegate's personal signature key").

Brickell and Sudia do not explicitly teach concatenating the predetermined data, first and second inforamtion and the first private key.

It would have been obvious to one of ordinary skill in the art at the time of the invention to concatenate the predetermined data, first and second information and the first private key.

The prior art Brickell and Sudia include each element claimed (delegate and delegator ID, predetermined data, and private key) and one of ordinary skill in the art could have combined the elements as claimed by known methods (concatenation) and that in combination, each element merely would have performed the same function as it did separately. One of ordinary skill in the art would have recognized that the results of the combination were predictable.

Claims 9 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brickell and Sudia further in view of Garay (6839436) .

Regarding Claims 9, 18

Brickell and Sudia teach the system and method claimed in claim 1. Brickell does not explicitly teach comprising loading predetermined data and a signature program including at least part of said cryptographic algorithm from at least one server connected to said terminal of said given first member before verification of said predetermined data by said given first member.

As disclosed in the rejection of Claim 1, Brickell teaches a Delegation Credential Service Provider, where upon authenticating the delegate predetermined data is transferred to the delegate. *("With the returned credential information, the relying party authenticates the delegate….based on the authentication result, the relying part generates…a service response and sends…the response back to the delegate" Paragraph [0033]).*

Garay teaches "In general, broadcast encryption techniques are employed to encrypt digital content to ensure that only privileged users are able to recover the content from an encrypted broadcast" Column 1 lines 12-16.

It would have been obvious to one of ordinary skill in the art at the time of the invention to send encrypted predetermined data to the delegate instead of loading before verification of said predetermined data.

The motivation to send encrypted predetermined data to the delegate is to perform the authentication at the delegate. The concept of broadcast encryption where data is sent first and then decrypted at the receiver is well known in the art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KRISTINE KINCAID can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139